Technische und organisatorische Maßnahmen (TOM) gemäß Art. 32 DSGVO

Organisationsbeschreibung

- Öffentlich -

Geltungsbereich:

DVV mbH

Als ein flexibles und innovatives Energiehandels- und Dienstleistungsunternehmen ist der Stadtwerke Duisburg Energiehandel Dienstleistungspartner für Stadtwerke und Weiterverteilerunternehmen in Deutschland. Wir verstehen uns als Dienstleister in einem KRITIS-Konzern und müssen ein dem Risiko angemessenes Schutzniveau mit geeigneten technischen und organisatorischen Maßnahmen (TOM) gewährleisten. Dieses unterliegt stetiger Veränderung und erfolgt nach dem sog. Stand der Technik.

Die EU-Datenschutz-Grundverordnung fordert

- die **Pseudonymisierung** und **Verschlüsselung** personenbezogener Daten (Art. 32 Abs. 1 lit. a)
- die Fähigkeit, die **Vertraulichkeit**, **Integrität**, **Verfügbarkeit** und **Belastbarkeit** der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen (Art. 32 Abs. 1 lit. b)
- Die Fähigkeit, die **Verfügbarkeit** der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen (Art. 32 Abs. 1 lit. c)
- ein **Verfahren** zur regelmäßigen **Überprüfung**, Bewertung und Evaluierung der **Wirksamkeit** der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.
  (Art. 32 Abs. 1 lit. d)

Wir ergreifen Maßnahmen bezüglich

A. Pseudonymisierung und Verschlüsselung

Neben pseudonymisierten Daten werden auch anonymisierte Daten nach Prüfung des geeigneten Verschlüsselungsverfahrens eingesetzt (z.B. bei Statistiken und Testdaten). Die Schlüssellänge ist angemessen gegenüber dem Schutzbedarf, insbesondere bei sensiblen Daten.

B. Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit

Die vier Schutzziele gewährleisten wir in Bezug auf die IT-Systeme und auf diesen laufende bzw. durch diese erbrachten Dienste. Erst dadurch wird der Schutz der personenbezogenen Daten erreicht.

B.1 Vertraulichkeit

B.1.1 Zutrittskontrolle: z.B. durch bauliche Maßnahmen wie einbruchshemmende und durch Zutrittskontrollsysteme gesicherte Türen inkl. Zutrittsberechtigungskonzept. Es existieren Sicherheitszonen, die weitere technische Maßnahmen enthalten. Organisatorisch ergänzt die Perimeterabsicherung inkl. Wachpersonal und der Zugang zu den Schließmitteln nur für Berechtigte. Der Zutritt und sowohl die Einräumung als auch der Entzug der Schließmittel wird protokolliert.

B.1.2 Zugangskontrolle: Aus der Ferne kann auf Daten in vernetzten Systemen nicht zugegriffen werden. Mittels Rechtemanagement erfolgt ein Zugang nur für Personen, die es für die Erfüllung ihrer Aufgaben benötigen. In Abwesenheit wird dieser Zugang gesperrt. Dazu werden die Mitarbeiter geschult und ohne Nutzerinteraktion erfolgt eine automatische Sperre. Es existieren zur Authentifizierung verschiedene Mehrfaktor-Techniken (Besitz, Wissen, biom. Merkmale). Passwörter haben eine hinreichende Komplexität und Länge.

B.1.3 Zugriffskontrolle: Nur Berechtigte können basierend auf einem Rollen- und Rechtemanagement auf Daten zugreifen und diese nicht unbefugt verarbeiten (lesen, verändern, kopieren, entfernen). Systeme sind mandantenfähig.

B.1.4 Weitergabekontrolle: Daten werden nur an diejenigen weitergegeben, für die sie bestimmt sind (Rollenmanagement plus starke Authentifizierungsverfahren). Auf dem Transportweg müssen die Daten verschlüsselt sein. Es ist eine Anomalie-Erkennung im Einsatz.

B.2 Integrität

Laufende Erkennung und Abwehr von Eingriffen (z.B. SIEM, IDS, Firewalls, Virenscanner) und entsprechende vorbeugende Maßnahmen (u.a. Patchmanagement).

B.3 Verfügbarkeit (im Sinne der Vorfallvermeidung)

Verwendung von unterbrechungsfreier Stromversorgung, NEA und Notstromgeneratoren. Moderne (stellenweise automatische) Brandschutz- und Meldeanlagen sind im Einsatz.

B.4 Belastbarkeit

Sinnvoll überdimensionierte Planung (z.B. Bandbreite gegen DoS-Attacken, Server- und Rechenkapazitäten auf Abruf), DDoS-Mitigations-Leistungen (Dienstleister) und redundante Systeme (Netzteile, Datenspeicher).

C. Verfügbarkeit (im Sinne der Vorfallbewältigung)

Bezogen auf die Verfügbarkeitsrisiken und die maximal tolerierbare Ausfallzeit (MTA bzw. MTPD) wird auf ein Business Continuity Management zurückgegriffen inkl. der Struktur, Konzepte und Überprüfung von Maßnahmen. (Wiederherstellungs)Übungen ergänzen.

D. Wirksamkeit

Die Absicherungsmaßnahmen werden aufgrund des risikobasierten Ansatzes nach dem Stand der Technik ständig geprüft und angepasst. Es wird sich nach ISO 27001 auf Basis IT-Grundschutz orientiert. Audits und Pen(etration) Tests werden auch bei Dritten beauftragt. Hierfür existieren klare Verantwortlichkeiten. Verantwortung, Planung und Umsetzung werden dokumentiert (auch bei Unterauftragnehmern).